# DATA PROTECTION

## for small and medium-sized businesses

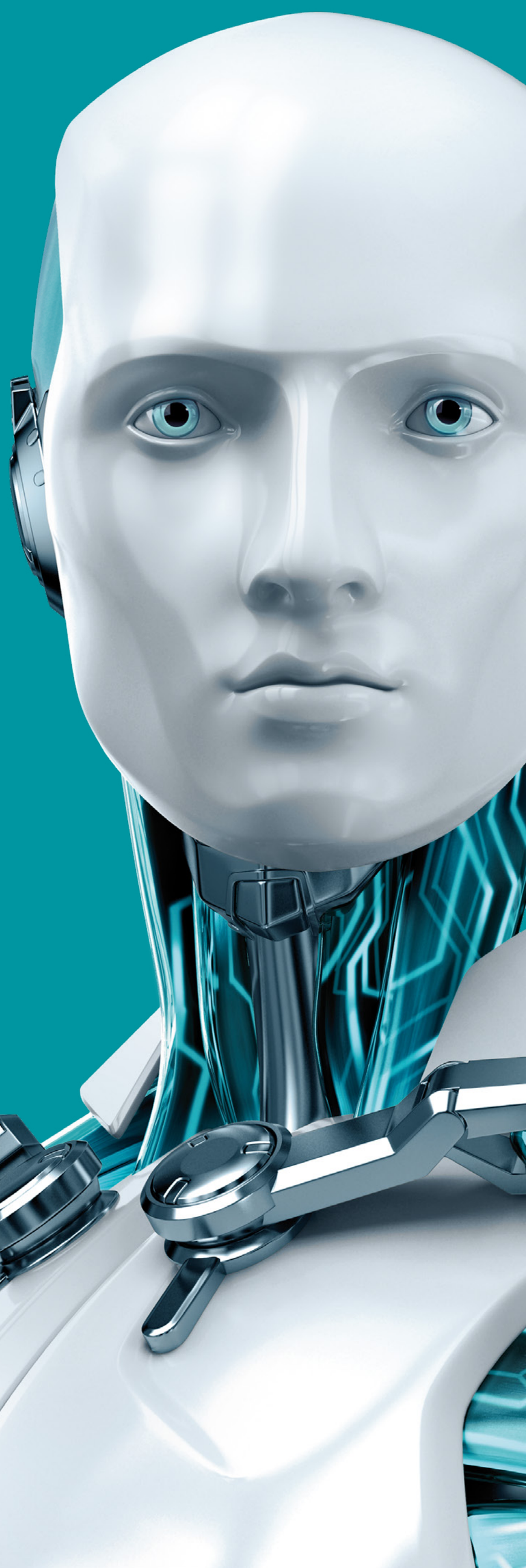
- Understand today’s threat landscape
- Find measures to protect your small/medium-sized business
- Minimize the impact of a data breach

CYBERSECURITY
EXPERTS ON YOUR SIDE

# #1 ENDPOINT SECURITY PARTNER FROM THE EUROPEAN UNION

**For more than 30 years, ESET® has been developing industry-leading IT security software and services, delivering instant, comprehensive protection against evolving cybersecurity threats for businesses and consumers worldwide.**

ESET is privately owned. With no debts and no loans, we have the freedom to do what needs to be done for the ultimate protection of all our customers.



## ESET IN NUMBERS

**110m+**
users worldwide

**400k+**
business customers

**200+**
countries & territories

**13**
global R&D centers

www.eset.com

# CONTENTS

# INTRODUCTION

"Your business is too small to attack" – said no hacker, ever! Cybercriminals are opportunistic predators, so while they may not specifically target your small or medium-sized business, if your company is connected to the internet in any way, for any purpose, they can find you. If your company's network, servers, applications, data, desktops, laptops, and mobile devices aren't properly protected, they can be breached. While a breach may not result in "15 minutes of shame" on the BBC or CNN à la Bupa, CEX, Clarkson, Equifax, Target, Uber, or Yahoo!, it will certainly have a serious impact – perhaps enough to put your company out of business. Security is becoming more and more a unique selling point. This book is your starting point for better digital business.

Although data breaches and cyberattacks aren't new, many of the techniques and tactics used by modern cybercriminals are – and they're particularly well-suited to the target-rich environment of small and medium-sized businesses (SMBs) that comprise more than 95 per cent of all businesses worldwide, employ more than half of the global workforce, and contribute more than half of the global economy's gross domestic product (GDP). Newer attack methods include:

- Advanced malware techniques (such as polymorphism and metamorphism), ransomware, and remote access Trojans (RATs).
- Directory harvest attacks (DHA) and targeted spam and phishing (spearphishing) email campaigns.
- Massive automated botnets.
- Domain Name System (DNS) hijacking and DNS cache poisoning.
- Port hopping and secure sockets layer (SSL) hiding.
- Distributed denial-of-service (DDoS) attacks.

Security threats are a more serious and frequent problem than ever before, and SMBs, which often run lean IT operations with limited budget and staff, are often easy targets for cybercriminals. At the same time, the fact that SMBs are, by definition, smaller than large enterprises and generally have fewer connected devices means that they can be more flexible and agile when defining and implementing a data protection strategy. If they take the right steps, SMBs can make themselves much less attractive targets for potential attackers.

In this book you will learn about the security technologies, tools, and processes that you need to help improve the ability of your company to protect its data and IT resources, and effectively minimize the impact of a data breach.

# About This Book

*Data Protection for Small and Medium-Sized Businesses* consists of six short chapters:

1. Cyberattacks and trends, the regulatory landscape, and the business impact of a breach
2. How to evaluate different data protection technologies, deployment options, and service models
3. The risk assessment process: identifying your assets, analyzing threats, and assessing vulnerabilities
4. Different data protection technologies, such as encryption, endpoint protection, firewalls, and more
5. Important organizational and process controls that are necessary to ensure effective data protection
6. Ten keys to effective data protection for small and medium-sized businesses

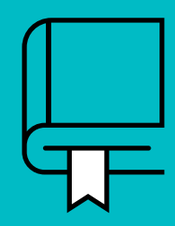
At the end of the book is a glossary to help you quickly decode any unfamiliar acronyms or terms.

# Assumptions

This book assumes you're an IT professional working for a small or medium-sized business. You may be the manager of a small, "jack of all trades" all-purpose IT team – or you may be the entire IT team yourself! You and your team are responsible for everything from changing toner cartridges and setting up user endpoints, to managing your company's network and dealing with security issues. As such, your job requires a broad range of IT knowledge and experience, but there are perhaps some areas – such as security and data protection – where your knowledge and experience are not as deep as you'd like.

# Icons Used in This Book

Throughout this book, special icons are used to identify important information.



**REMEMBER**

*This icon denotes information that you should commit to memory, as you will need it in future*

**TIP**

*This icon points out particularly useful nuggets of information and helpful advice*

**WARNING**

*These alerts offer practical advice to help you avoid potentially costly or frustrating pitfalls*

# Beyond the Book

There's only so much that a short book can cover, so if you find yourself thinking "Where can I learn more?", just go to www.eset.com

**In This Chapter**

- Measuring the true cost of a data breach
- Looking at the modern threat landscape
- Learning from past breaches
- Understanding compliance mandates

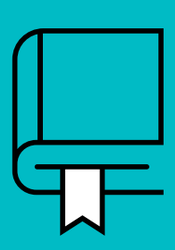
Chapter 1

# RECOGNIZING THE DATA PROTECTION IMPERATIVE

*In this chapter, you will learn how a data breach can impact your business, how the modern threat landscape has evolved, how recent data breaches have impacted other small and medium-sized businesses (SMBs), and what changing legal and regulatory requirements mean for your business.*

## Understanding the Business Impact of a Breach

Small and medium-sized businesses (SMBs) represent 99 per cent of all businesses in the EU and more than 95 per cent of businesses worldwide, thus it shouldn't be surprising that SMBs are victims of more than 70 per cent of security breaches, according to the International Data Corporation (IDC). Yet many businesses believe that they're not vulnerable to cyberattacks because of their small size and limited assets. Unfortunately, this is not the case.



REMEMBER

*According to the Verizon 2017 Data Breach Investigations Report (DBIR), the focus of attacks (specifically, point-of-sale intrusions) has shifted to restaurants and small businesses. Further, three-quarters of victims of the top six threat actions – stolen credentials, backdoors, spyware, phishing, data exfiltration, and command-and-control (C2) malware – are web-based, non-retail small businesses.*

In the UK, insurance company Zurich reports that more than 875,000 small and medium-sized businesses were affected by a cyberattack last year, at a cost of more than $13,000 for over a fifth of those businesses, and more than $69,000 for one in ten. By comparison, the Ponemon Institute's 2017 Cost of a Data Breach Study found that the average total cost of a data breach for large enterprises is approximately $3.62 million.

According to the findings of a study regarding the global cost of data breaches, the average cost of data breaches more than doubled between 2014 and 2015, while the average cost for each lost or stolen record increased slightly to almost €150. This suggests that the overall the cost of a data breach has not fluctuated significantly over the years; thus, it is a permanent cost which organizations need to be prepared to deal with and incorporate into their data protection strategies.

While the cost of a breach for SMBs is significantly less than the cost for large enterprises, SMBs typically don't have the resources – financial or otherwise – to respond to and recover from a major data breach. With regulations such as the EU's General Data Protection Regulation (GDPR) requiring businesses – regardless of size – to be able to forensically explain exactly what happened in the event of a breach, the impact of a breach for SMBs is likely to be far costlier going forward.

**TIP**

*Cyber insurance is a great way for SMBs to mitigate the cost of a cyberattack or data breach. However, cyber insurance won't protect you from an attack or breach and it is NOT an alternative to implementing security best practices, policies, controls, and technologies.*

The full cost of a security breach includes:

- Business disruption (including lost time and productivity)
- Direct costs (such as notifications, customer support, credit monitoring services, customer retention incentives, restitution, and card replacement)
- Loss of customers (churn rate), brand damage, and loss of reputation
- Litigation from consumers, business partners, and investors.
- Regulatory fines and penalties
- Recovery and forensic costs (these can account for the major part of costs)
- Lost assets (such as intellectual property)

**WARNING**

*According to the National Cyber Security Alliance, 60 per cent of small businesses will go out of business within six months of a cyberattack.*

# Surveying the Current Threat Landscape

The number, magnitude, and cost of data breaches will continue their upward trajectories for the foreseeable future. These attacks will be underpinned by several trends that will continue to loom large for businesses of all sizes:

**Automated attacks on a massive scale** are becoming the modus operandi for cybercriminals who leverage sophisticated malware and botnets to breach any vulnerable organization or network, rather than targeting specific businesses. If you're connected to the internet, you will be found one day. Nobody is a target, but everyone can be a victim.

**Ransomware** will continue to be a growing menace. According to research by Datto, approximately 5 per cent of all SMBs worldwide were victims of ransomware attacks over the past year. Thirty-five per cent of managed service providers (MSPs) reported that small business victims pay the ransom, 15 per cent of whom do not recover their data.

**Crime-as-a-service (CaaS)** will expand as criminal organizations make their malicious wares increasingly sophisticated. Criminal groups are making forays into new markets and commoditizing their activities globally, which will result in more persistent and damaging cybersecurity incidents than ever before. The barriers to entry are also much lower, with cyberweapons such as ransomware-as-a-service and malicious sites (like nulled.to) making cybercrime more accessible to aspiring, low-skilled cybercriminals.

**The internet of Things (IoT)** will add unmanaged risks as organizations embrace IoT devices but, in the rush to market, lose sight of the fact that these devices are often insecure by design, thus affording ample opportunities for attacks. Consider too what heavy data carriers mobile devices are.

**Cloud computing** enables SMBs to compete with the "big boys" as smaller businesses can have access to the same powerful computing resources as larger enterprises, while forgoing large capital IT expenditures and costly IT support. According to the UK-based consulting and cloud solutions firm BCSG, approximately two-thirds of SMBs are already using an average of three cloud-based software-as-a-service (SaaS) applications. Typical SaaS applications for SMBs include customer relationship management (CRM), online collaboration, data storage, online marketing, contract management, and supply chain software. While these types of solutions are usually inherently more secure than similar on-premises solutions, businesses must still ensure that their cloud service providers – particularly in smaller markets or in the case of boutique SaaS applications – follow security best practices, comply with relevant regulations (such as GDPR), and meet acceptable service-level agreements (SLAs). For the SMBs' part, the cloud does not obviate ultimate responsibility for the security and privacy of sensitive data and regulatory compliance. SMBs must ensure strong identity and access management, secure authentication to cloud services, and proper configuration, operation, and maintenance of cloud-based servers (in the case of infrastructure-as-a-service, or IaaS).

**The supply chain** will continue to be targeted as a backdoor into companies by exploiting vulnerabilities in upstream and downstream supply chain partners who share valuable and sensitive information. Remember that you too are a supply chain to your customers.

**Regulation** adds complexity, and businesses may have their attention and investments drawn away from other important security initiatives due to the additional resources required to address compliance requirements (discussed later in this chapter).

For SMBs, these trends – and the lack of orchestration between all of these trends – are particularly bad news. Typically lacking the financial and information security resources of larger enterprises, SMBs represent a "sweet spot" for cybercriminals (see Figure 1-1). It's not only cybercriminals wreaking havoc: also worth a mention are unintentional breaches by insiders.

**WARNING**

*The Information Security Forum (ISF) notes that the increased pervasiveness of data breaches and the higher volume of impacted records are expected to result in far higher costs for organizations of all sizes.*

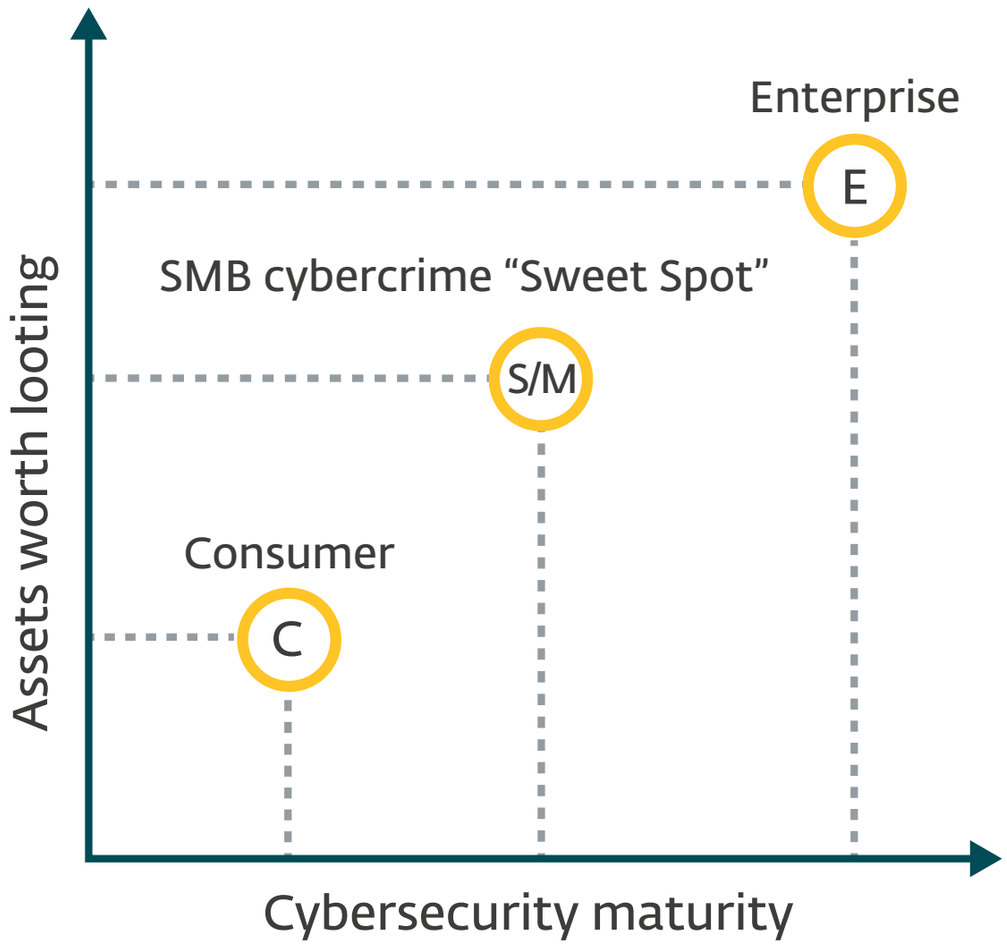
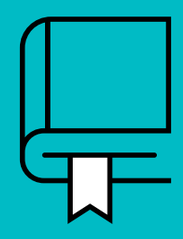



**Figure 1-1:** SMBs are typically a more valuable target than consumers and a more vulnerable target than large enterprises.

# Looking at Recent Data Breaches and Leaks

Although major cybersecurity breaches involving large enterprises and sensitive data seem to get all the sensational news coverage, cyberattacks and breaches involving SMBs are no less frequent and damaging. In fact, given the relative number of SMBs and their limited financial and security resources compared to larger enterprises, the impact of a cyberattack or data breach on an SME's customers – as well as for the viability of the SME itself – can be far more damaging.



REMEMBER

*Small businesses (fewer than 50 employees) and small office-home office (SOHO) businesses get less sensational news coverage than larger businesses but are no less vulnerable to cyberattacks and breaches.*

Some recent examples of SME data breaches and cyberattacks include:

### Obike

In December 2017, it was reported that as early as June 2017, Obike, a Singapore-based company that offers bike sharing services in several cities throughout Asia Pacific, Europe and the UK, was the victim of a data breach involving sensitive customer information including names, contacts, profile photos, and location.

### TIO Networks USA

In December 2017, it was reported that TIO Networks USA, a Canadian payment processing service recently bought by PayPal Holding of California, had been the victim of a data breach involving the personal and financial information of approximately 8,000 City of Tallahassee (Florida) utility customers.

### Longs Peak Family Practice

In November 2017, Longs Peak Family Practice, a Colorado-based medical clinic, discovered a data breach that potentially compromised patients' names, birth dates, phone numbers, email addresses, social security numbers, driver's license numbers, insurance, and other sensitive information.

### Royal National Institute of Blind People (RNIB)

In November 2017, UK-based RNIB was the victim of a data breach involving the credit and debit card details of 817 customers in its online charity shop.

### Chilton Medical Center

In October 2017, New Jersey-based Chilton Medical Center discovered that a former employee had sold a stolen hard drive containing protected health information (PHI) on 4,600 patients.

WARNING

*According to the Verizon 2017 Data Breach Investigations Report (DBIR), 60 per cent of data breach cases involve insider data theft.*

### London Bridge Plastic Surgery and Aesthetic Centre (LBPS)

In October 2017, it was reported that LBPS had been the victim of a data breach potentially involving sensitive patient data and photographs.

### Colorado Center for Reproductive Medicine (CCRM)

In October 2017, CCRM Minneapolis (Minnesota) was the victim of a ransomware attack that potentially affected the protected health information (PHI) on nearly 3,300 patients.

### Heritage Valley Health Systems

In June 2017, Heritage Valley Health Systems, a healthcare network that manages two hospitals and numerous acute, ambulatory, and ancillary care services throughout Western Pennsylvania, was the victim of a global ransomware attack that impacted patient services.

## Addressing the Changing Legal and Regulatory Frameworks

With hundreds of regulations worldwide mandating information security and data protection requirements, businesses of all sizes are struggling to achieve and maintain compliance. Some examples of these regulations and standards include:

### EU General Data Protection Regulation (GDPR)

Applicable to any organization that does business with EU citizens. This regulation strengthens data protection for EU citizens and addresses the export of personal data outside the EU.

### Swiss Federal Data Protection Act (“DPA”)

Switzerland has recently updated its 1992 Federal Act on Data Protection (FADP) to maintain parity with GDPR requirements. These updates modernize Swiss data protection laws to maintain Switzerland’s adequacy status granted by the European Commission and ensure the free flow of data from the EU into Switzerland and vice versa. Other EU countries are similarly updating their data protection laws in the wake of the GDPR.

### South Africa Protection of Personal Information (PoPI) Act

Ensures that South African institutions collect, process, store, and share personal information about another entity responsibly, and bestows certain rights of protection and control to individuals as the owners of their personal information.

### US Health Insurance Portability and Accountability Act (HIPAA)

Applicable to any organization that processes or stores PHI. It protects patient confidentiality and data privacy.

### Canada Personal Information Protection and Electronic Documents Act (PIPEDA)

Applicable to organizations that do business with Canadian citizens. This regulation protects the privacy of personal information for Canadian citizens.

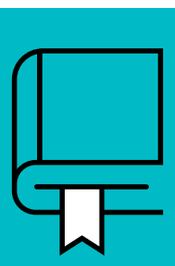
### International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC) 27000 family of standards

Internationally adopted information security standards including: Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001), Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002), Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017), and Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018).

### Payment Card Industry (PCI) Data Security Standards (DSS)

Applicable to any business that accepts, processes, or stores payment card (such as credit, debit, and cash card) transactions.

While these and other regulations are enacted to ensure that appropriate security and data protection best practices are implemented within organizations that handle sensitive data, they're often complex, ambiguous, and costly to address. Unfortunately, this has the unintended consequence of leading many organizations to focus their efforts on regulatory compliance rather than information security and data protection.



REMEMBER

*Compliance and security are not the same thing.*
*An organization can be compliant, but not secure. Conversely, an organization can be secure, but not compliant.*

GDPR is designed to protect the privacy of EU individuals by giving them greater control and rights over their personal data. Individuals can, for example:

- Request that businesses provide a copy of their data in a structured, commonly used, and machine-readable format
- Have their data transmitted to another controller (the "right to data portability")
- Have their information deleted (the "right to be forgotten")

GDPR implements much stricter rules regarding consent, notification of data breaches, mandatory privacy impact assessments, and the requirement for “privacy by design and by default.”

Failure to comply with GDPR can result in fines of up to 4 percent of a business’s annual worldwide revenue, or €20 million (more than $24 million) – whichever is greater.

GDPR also suggests a number of technical security measures that can be used to achieve data protection, including:

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services processing personal data
- The ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring personal data processing security

To learn more about GDPR and the security measures that your company can take to achieve GDPR compliance, go to https://encryption.eset.com/

# FIVE STEPS TOWARDS GDPR COMPLIANCE FOR SMALL AND MEDIUM-SIZED BUSINESSES

1

## Establish and assess how you deal with data

A thorough understanding of how your organization deals with data is paramount. Under previous rules, only data controllers were liable for compliance, but GDPR obligations fall on data handlers too. You need to establish whether your organization is a data processor or a data controller, bearing in mind that it could be both. Knowing where data is stored and that location's security, as well as determining whether that data is being shared, is critical.

2

## Learn from the past

To check your capabilities in terms of reacting to a future attack, examine what has happened during past breaches and question whether the steps taken can meet the new requirements set by the GDPR. Under the new rules, breaches must be reported within 72 hours, together with information about the severity of the attack. If your company is unable to do so, that shortcoming may result in a hefty fine. Updating (or creating) your incident response plan and regularly testing your incident response capabilities and effectiveness is a critical step toward ensuring GDPR compliance.

3

## Appoint a data protection officer or someone with formal responsibility for data protection

This may be simple advice for a company with lots of money, but the added expense makes this off-putting for smaller businesses. However, it's not as off-putting as being fined 4 percent of your revenue and might not need to be a full-time responsibility. The data protection officer acts independently and, reporting to the highest level of management, should help to implement the requirements. Allocating further resources sooner rather than later will ensure that your company is not only compliant, but also is equipped to deal with any data breach and mitigate the possibility of being fined.

4

## Educate your staff, and yourself, on the rules

One of GDPR's main aims is to strengthen the ability for people to be forgotten and have their data deleted. Companies will also have to gain "clear affirmative action" from individuals before processing their data. The rules also make it harder for children to hand over their data. Knowing how the rules change your organization's handling of consent, and the rights of individuals, is imperative.

5

## Know your lead supervisory authority

The authority that handles any complaint against your company depends on where your company is based, not on the location of the individual raising the complaint. This can be difficult for companies that operate internationally, or even have multiple sites in different regions. There are also other directives in different countries that may go further than GDPR that also need to be considered.

**In This Chapter**

- Learning the fundamentals of data protection
- Deploying on-premises and in the cloud
- Choosing managed services and outsourcing

Chapter 2

# GETTING STARTED WITH DATA PROTECTION

*In this chapter, you will learn the basics of data protection technology, compare different deployment options on-premises and in the cloud, and explore managed security service providers and outsourcing options.*

## Understanding the Basics of Data Protection

Protecting the security and privacy of sensitive customer information is a core obligation of all businesses, including SMBs.

Data protection (and more broadly, information security) encompasses all the administrative, logical, and technical controls necessary to protect information. The C-I-A triad (see Figure 2-1) is commonly used to guide the development and implementation of a framework for managing information security within an organization. The C-I-A triad consists of three fundamental information security concepts:

### Confidentiality (and privacy)

Prevents the unauthorized access, use, disclosure, perusal, inspection, or recording of data.

### Integrity

Prevents the unauthorized or improper modification of data.

### Availability

Ensures that authorized users have reliable and timely access to data and prevents the unauthorized disruption or destruction of data.


**Figure 2-1:** The C-I-A triad.

For example, to protect the confidentiality of sensitive data, various employment, security and privacy policies typically define who has access to certain data within an organization, for what purposes, and what they are authorized to do with that data. Technical controls to ensure confidentiality might include identity and access management (IAM), encryption, and data loss prevention solutions.

To protect the integrity of data, various technical solutions such as checksums and data input validation in forms and databases may be implemented. Digital signatures and hashing use encryption technologies to prove the authenticity of data, or to verify that data hasn't been altered. Finally, anti-malware solutions protect the integrity of data (and potentially the confidentiality and availability of data).

To protect the availability of data from accidental (for example, deletion) or intentional (for example, a ransomware attack) destruction, backup and recovery systems, as well as backup and retention policies, are implemented. Data protection technologies are discussed further in Chapter 4.

Effective information security requires a business to address the confidentiality, integrity, and availability of all of its sensitive data, including the systems and applications that process and store that data.

Using a risk-based approach, organizations can implement appropriate controls to address vulnerabilities and achieve an acceptable level of risk to data against specific threats. The higher the risk to the data, the greater the protective measures that should be implemented. Security risk management consists of four key phases (see Figure 2-2)


**Figure 2-2:** A basic risk management process.

## Risk assessment

There are many risk assessment methodologies with varying levels of cost and complexity. The basic process consists of:

- **Asset identification**
  Identify all the organization's assets (both tangible and intangible) which require protection, including the asset's quantitative (such as cost or contribution to revenue) and/or qualitative (such as relative importance) value.
- **Threat analysis**
  Define possible adverse natural and/or manmade circumstances or events, the potential impact or consequences, and the likelihood and frequency of occurrence.
- **Vulnerability assessment**
  Determine what safeguards and/or controls are absent or weak in an asset, thereby making a threat potentially more harmful, costly, likely, or frequent.

## Risk treatment

The risk assessment provides the basis for management decisions regarding what to do about specific risks. Options include:

- **Risk mitigation**
  Implementing policies, controls, and/or other measures to reduce the impact or likelihood of a specific threat against a specific asset.
- **Risk assignment (or transference)**
  Transfer the potential risk to a third party, such as an insurer, a service provider, or other agent that explicitly agrees to accept the risk.
- **Risk avoidance**
  Eliminate the risk altogether, for example by upgrading or disposing of the asset, or ceasing the activity that introduces the risk.

## Risk acceptance

This is the formal management approval of the risk treatment measures that are implemented, and the acceptance of any residual (or remaining) risk that cannot be further or practically mitigated, assigned, or avoided.

## Risk communication

Appropriate stakeholders need to be made aware of any risk treatment and/or risk acceptance decisions that have been made, including their individual roles and responsibilities with regard to specific risks.

# Comparing On-Premises, Cloud, and Hybrid Deployment Options

Businesses today have many options for deploying technology, including on-premises, in the cloud, and a hybrid deployment with some resources located on-premises and others located in the cloud.

In the not-too-distant past, the only deployment option for businesses was on-premises. Even the smallest of businesses often found themselves needing to purchase several expensive servers, often precariously installed in a dark, crowded cupboard somewhere in the building (perhaps with a fire sprinkler in the ceiling – just in case a fire didn't destroy your expensive IT investments). These servers required ongoing administration and maintenance, which often meant additional IT staff or contractors. Not only servers, but also networking equipment such as routers, switches, and network cabling had to be installed and managed. At a minimum, a firewall protected the "trusted" internal network from the "untrusted" internet.

Managing an on-premises server room or data center is still a viable option for many businesses. But as virtualization, network connectivity, and cloud computing technologies have become more robust and stable over the past decade, many businesses are now moving some or all of their IT resources to the cloud.

But what exactly is the cloud? Practically every technology vendor in the market has a "cloud" offering of some sort and, unfortunately, the definition of cloud can sometimes be a little, well, cloudy. So, to clear the air about the cloud, let's define a few important elements of the cloud using the vendor-neutral US National Institute of Standards and Technology (NIST) definitions. According to NIST, the three cloud computing service models are as follows:

### Software as a Service (SaaS)

Customers are provided access to an application running on a cloud infrastructure. The application is accessible from various client devices and interfaces, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer may have access to limited user-specific application settings, and the security of the customer's data is still the responsibility of the customer.

### Platform as a Service (PaaS)

Customers can deploy supported applications onto the provider's cloud infrastructure, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over the deployed applications and limited configuration settings for the application-hosting environment. The company owns the deployed applications and data and is therefore responsible for the security of those applications and data.

### Infrastructure as a Service (IaaS)

Customers can provision processing, storage, networks, and other computing resources and deploy and run operating systems and applications, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over operating systems, storage, and deployed applications, as well as some networking components. The company owns the deployed applications and data and is therefore responsible for the security of those applications and data.

**TIP**

*The different cloud service models (SaaS, PaaS and IaaS) have different security implications for customers. For example, SaaS offerings such as Microsoft 365 and Salesforce provide infrastructure security through the cloud provider, but data security and authentication are the customer's responsibility. The customer's security responsibilities increase progressively in PaaS and IaaS offerings. Many cloud solutions shift the focus from application or infrastructure security to authentication and data integrity security.*

NIST also defines four cloud computing deployment models:

### Public

A cloud infrastructure that's open to use by the public. It's owned, managed, and operated by a third party (or parties) and exists on the cloud provider's premises.

### Private

A cloud infrastructure used exclusively by a single organization. It may be owned, managed, and operated by the organization or a third party (or a combination of both), and may exist on or off premises.

### Hybrid

A cloud infrastructure composed of two or more of the other deployment models, bound together by standardized or proprietary technology that enables data and application portability.

### Community (not common)

A cloud infrastructure that's used exclusively by a specific group of organizations.

The journey to the cloud often begins like many new initiatives, with non-production or non-critical applications and systems, such as a development environment or backup systems. As the journey continues, many businesses begin to "lift and shift" existing applications to the cloud and deploy new applications directly in the cloud. Finally, "cloud first" organizations make every effort to deploy as much of their IT environment to the cloud as possible and develop "cloud native" apps for their customers.

The many benefits of the cloud for businesses include:

### Greater agility and responsiveness

You can access applications and data in the cloud from anywhere, at any time, on any device.

### Faster time-to-market

You can develop and deliver new products and services more quickly in the cloud with PaaS or easily provisioned IaaS resources.

### On-demand scalability

Additional software licensing and/or infrastructure can be provisioned and deprovisioned as needed, which supports the needs of rapidly growing and cyclical businesses that may not be able to accurately predict market changes and business growth.

### Increased stability

Cloud infrastructure is typically installed in robust data centers built for performance, stability, and reliability, and managed by large teams of specialized IT staff.

### Reduced capital investments

You can deploy your entire IT infrastructure in the cloud and forgo costly capital investments. The cloud offers predictable "pay as you go" subscription-based services that allow you to budget your IT needs as an ongoing operating expense and only pay for what you use.

**WARNING**

*Moving your applications and data to the cloud doesn't eliminate or transfer your responsibility for the security of your applications and data. Although the cloud service provider is responsible for certain aspects of the environment, you are always ultimately responsible for protecting and securing your applications and data. Cloud service providers commonly refer to a "shared responsibility model" that clearly shows what they are responsible for in the cloud and what you are responsible for – and nowhere does the shared responsibility model ever show the cloud service provider being responsible for the security of your data!*

# Considering Managed Security Service Providers and Outsourcing

Keeping IT systems and applications secure, patched, protected, and compliant in the face of ever-growing risks and increasingly sophisticated threats is a challenging burden for businesses of all sizes. This is especially true for SMBs with limited IT staff and security resources. Many SMBs are turning to managed service providers (MSP) for the solution. The benefits and value of an MSP for SMBs include:

### Better control over the IT budget

MSPs can offer a full portfolio of products and services compared to the relatively limited internal resources of SMBs. Opting for the services of an MSP also leads to greater financial flexibility and more predictable costs, and with adjustable billing plans, SMBs also have better control over their IT and security budget.

### Trusted advisor with knowledge and experience

SMBs can leverage the deep knowledge and broad experience of IT and security staff employed by MSPs.

### Market focus and insight

MSPs that are focused on security have better insight into the security solutions available on the market and can provide custom security offerings for their customers.

### Innovation

Specialized MSP security teams can make adopting and implementing innovative solutions easier and help customers to keep pace with current market developments.

### Prepared for change

MSPs enable their clients to add or remove any software or hardware according to their current needs without having to go through the painstaking process of acquiring, implementing, and maintaining new hardware and software resources.

# SHEFFIELD WEDNESDAY CHAMPIONS ESET I.T. SECURITY

Sheffield Wednesday Football Club (SWFC) is one of the oldest professional clubs in the world. Hillsborough Stadium has been a host venue for both World Cup and European Championships, and FA Cup semi-finals. The Club has a strong community program that encourages people to participate in sporting activities and to maximize the community facilities at SWFC. A key part of the program is developing life skills, and SWFC has invested in computer equipment to enable it to operate portable classrooms, alongside more permanent facilities.

## Challenges

SWFC's antivirus software had become cumbersome and was using up too much processing power. SWFC also wanted a centralized admin console and automated updates to ensure that its 310 machines were protected from the latest threats to ensure business continuity.

## Solution

Since switching to ESET Endpoint Antivirus, Richard Ford, Head of IT, hasn't looked back. "ESET was just what we were looking for – light processing power, reliable protection, and cost scalable, yet easy to deploy and manage centrally. It doesn't distract us, or users, with issues such as slowdowns or false positives and works exactly how all antivirus should do, quietly in the background."

## Results

- Easily integrated, quietly operating security solution with a small footprint that doesn't choke network traffic
- Easy set-up and low maintenance
- A centralized admin console provides reliable threat protection for servers and workstations, giving central visibility and real-time insights
- The solution updates itself regularly once configured

**In This Chapter**

- Looking at the risk assessment process
- Identifying data processing operations
- Determining the impact of a data breach
- Identifying pertinent data security threats
- Implementing appropriate data protection controls

Chapter 3

# ASSESSING DATA SECURITY RISKS

*In this chapter, you will learn how to apply the risk management process (discussed in Chapter 2) to data security.*

## Understanding the Risk Assessment Process

Risk assessment is the first phase of the risk management process (discussed in Chapter 2). A risk assessment consists of:

- Identifying your assets (both tangible and intangible)
- Analyzing threats (including impact and likelihood)
- Assessing vulnerabilities (that is, what safeguards or controls are absent or insufficient in a given asset)

Similarly, assessing data security risks involves:

- Identifying your data processing operations (to determine how and where your data assets are used by your business)
- Determining potential business impact (if your data is compromised)
- Identifying possible threats and evaluating their likelihood of occurrence, including frequency
- Evaluating risk (to assess which safeguards or controls should be implemented to protect your data)

# Step 1
# Identify Your Data Processing Operations

Data within an organization has different risk profiles, not only based on the content of the data, but also due to the way data is used within the organization. Thus, it is important to understand how data is processed within your business as you begin the risk assessment process. For example, a typical SME might have some or all of the following types of data processing operations:

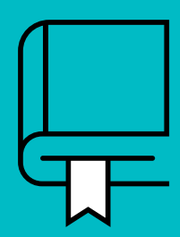
**Human resources** such as employee payroll management, recruiting and retention, training records, disciplinary actions, and performance evaluations.

**Customer management, marketing, and suppliers** such as customer information, purchase and sales orders, invoices, email lists, marketing and advertising data, and vendor contracts.

**Personnel safety and physical security** such as employee security access logs, visitor logs, and video monitoring.

For each data processing operation, consider the following:

- What personal data is being processed?
- What is the purpose of the process?
- Where does the processing occur?
- Who is responsible for the process?
- Who has access to the data?

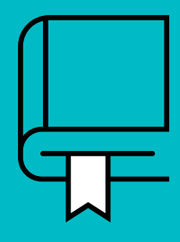


REMEMBER

*The principle of least privilege is an information security best practice in which end users are granted only the minimum level of access required to perform a specific job function.*

# Step 2
# Determine Potential Business Impact

Next, you need to determine the potential impact of a data breach or compromise. A breach or compromise may affect the confidentiality (for example, unauthorized access) of data, the integrity of data (for example, unauthorized modification), or the availability of data (for example, a ransomware attack).



REMEMBER

*Organizations must protect the confidentiality, integrity, and availability of data. In information security, this is known as the C-I-A triad (see page 14-15).*

In a typical risk assessment, the potential impact of a given risk is typically expressed in terms of damage to the organization, such as the loss or destruction of a physical asset (for example, a server, a copier machine, or a vehicle).

The impact of a risk to data security to the business is similar to other risk impacts, but the impact may be indirect. In the case of sensitive personal data, the individual whose data is breached or compromised is the direct victim. In such cases, an individual's identity or financial assets may be stolen and/or their privacy may be violated. The impact to the business is less direct but still very costly and may include (among others):

- Loss of customers and revenue
- Brand damage and adverse public relations
- Regulatory fines and litigation
- Breach notifications and credit monitoring services
- Forensic analysis and recovery



TIP

*Business impact can be classified as Low, Medium, or High. However, the actual definition of each of these impact levels will be unique to every business and should involve both objective (quantitative) and subjective (qualitative) measures.*

## Step 3
## Identify Possible Threats and Evaluate Their Likelihood

A threat can be any event or circumstance, either natural or manmade, that has the potential to negatively affect the confidentiality, integrity, or availability of personal or sensitive data. This can include cybersecurity attacks, accidental loss or disclosure, insider threats, fire and flooding, earthquakes and tsunamis, severe weather (such as a hurricane or tornado), civil unrest, labor disputes, and more. Businesses must identify possible threats to their data processing operations and evaluate the likelihood (including frequency of occurrence) of each possible threat. Ensure that you cover threats in well-defined areas including threats from network and technical resources (software/hardware) that are used for data processing, threats from related processes and procedures, threats from involved human resources, and threats from scale of processing.

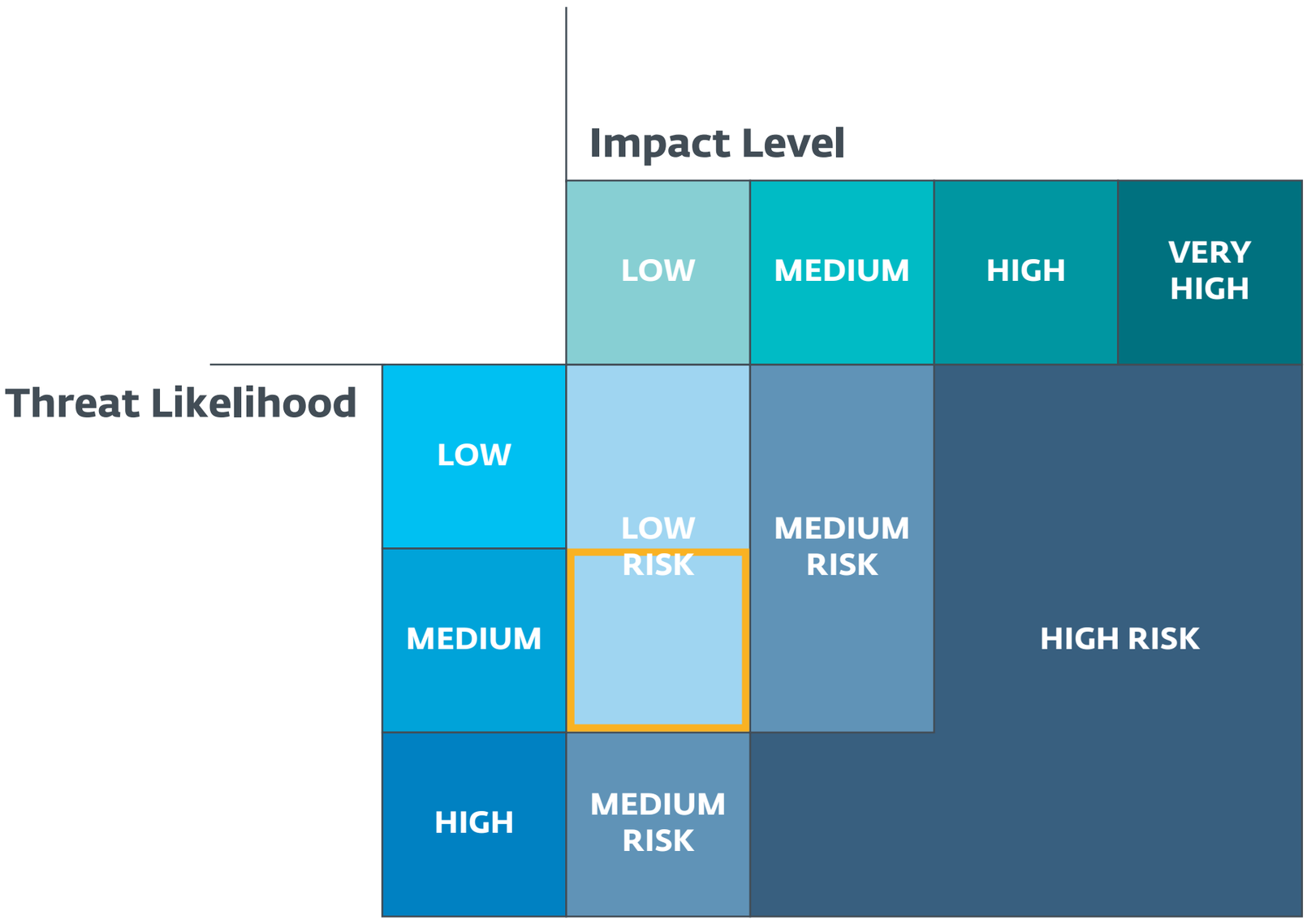
**TIP**

*For each threat identified, the likelihood can be classified in a manner similar to the business impact: Low, Medium, or High. When evaluating the likelihood of a threat occurring, consider both the likelihood of the threat occurring at all, as well as how frequently it is likely to occur during a given period (for example, over a one-year period).*

## Step 4
## Evaluate Risk

Once you've identified all of your data processing operations (and the data being processed), determined the potential business impact of a data breach or compromise, and identified possible threats and the likelihood and frequency of occurrence, you can evaluate the risk associated with each operation and determine the appropriate data protection control technology controls (discussed in Chapter 4) and organizational/process. According to the risk evaluation, organizational and process controls (discussed in Chapter 5) should be implemented to properly secure your data and data processing operations using a risk-based approach.

Figure 3-1 shows a data assessment template and an example of a data processing operation assessment.




## Threat Likelihood

For particular data processing operation walk through list of possible data processing threats and evaluate/score threat likelihood. Final likelihood should be based on sum of score from all threats in threat list.

- **Low** – the threat is unlikely to materialize
- **Medium** – there is a reasonable chance that the threat materializes
- **High** – the threat is likely to materialize

## Impact Level

For particular data processing operation evaluate possible impact om data confidentiality, integrity, availability (C-I-A triad). The highest impact of the three is the final impact level.

- **Low** – minor inconveniences, which could be overcome without any problem
- **Medium** – significant inconveniences, which could be overcome despite a few difficulties
- **High** – significant consequences, which could be overcome but with serious difficulties
- **Very High** – significant, or even irreversible consequences, may not be overcome

## Data processing operation poses

- **Low Risk**
- **Medium Risk**
- **High Risk**

## Example

**Data processing operation:** Marketing/Advertising
**Data processed:** Contact info
(e.g. name, postal address, telephone number, email)
**Data classification:** Personal Data
**Processing purpose:** Promotion of goods and special offers to possible customers
**Data Subjects:** Customers and leads

## Threat Likelihood

Network and technical resources (HW, SW) threats: Medium
processes and procedures threats: Low
involved human resources threats: Medium
Business sector and scale of processing threats: Medium
**Final likelihood: Medium**

## Impact Level

Impact level assessment confidentility: low, integrity: low, availability: low
**Final impact level: Low**

## Data processing operation poses

- **Low Risk** – processing of Marketing/Advertising data pose Low risk – Technical and Organizational measure adequate to this risk should be implemented.

**Figure 3-1:** Risk Assessment Matrix for data processing operation

**In This Chapter**

- Exploring data protection solutions
- Securing the network
- Reducing mistakes and improving efficiencies with orchestration

Chapter 4

# UNDERSTANDING DATA PROTECTION TECHNOLOGY

*In this chapter, you will learn about different information security and data protection technologies that you can consider implementing throughout your business – from the endpoint to the network and beyond.*

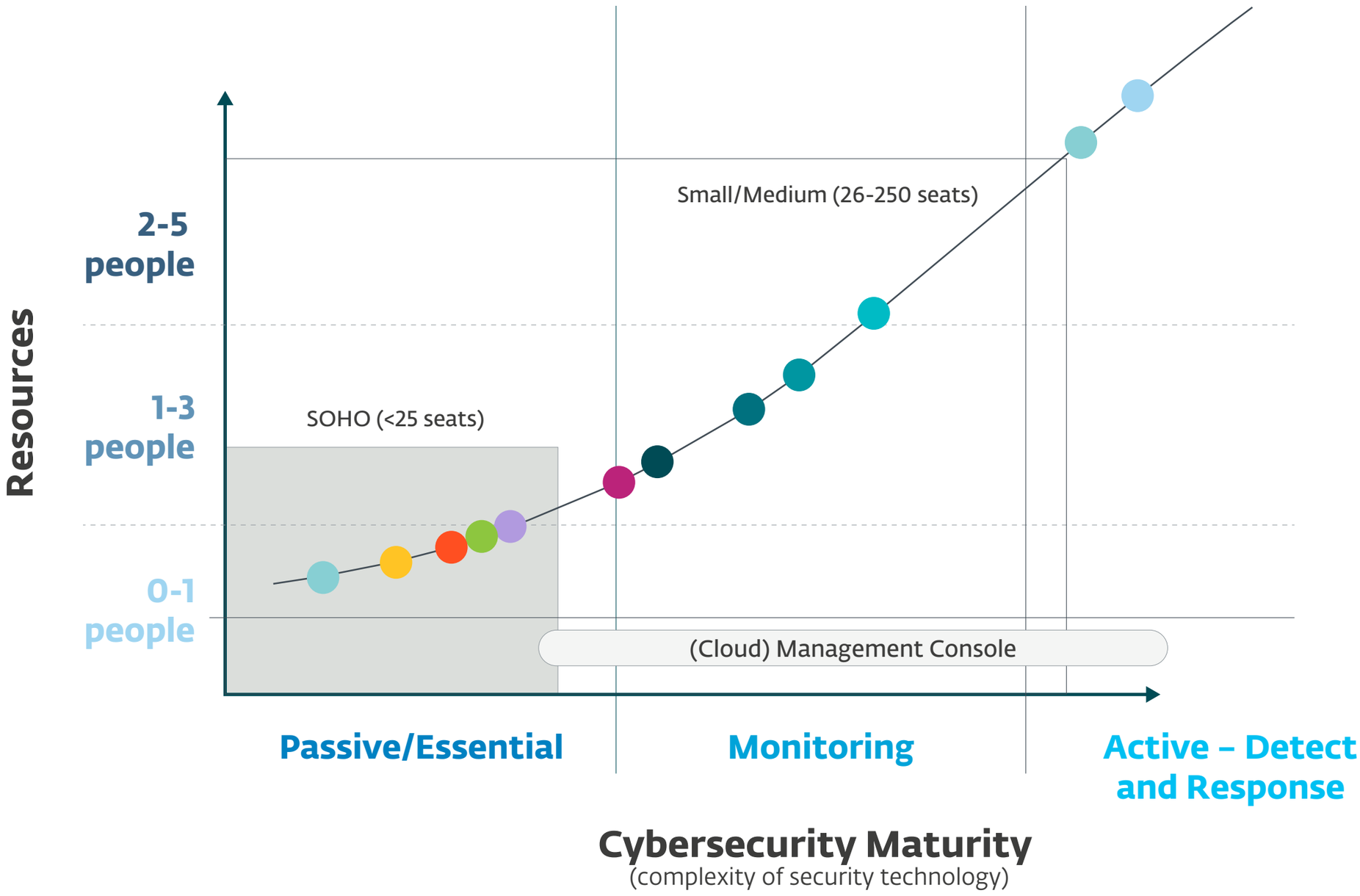
## Protecting Data Everywhere

Data is a critical asset, but it can pose a huge risk to your business. There are many security technologies you can use to protect data in your workspaces (such as computers and mobile devices), on your network, and on the backend (such as an on-premises server room or cloud-based datacenter). Figure 4-1 identifies various security technologies (discussed below) to consider implementing for your business, as appropriate for your level of risk and available resources.

Beyond anti-virus (A/V) software, SMBs should consider implementing:

### Endpoint protection

Extending beyond antivirus software, endpoint protection is multi-layered technology that prevents malware (including viruses, worms, ransomware, spyware, Trojans and remote access Trojans, and rootkits/bootkits) infections, vulnerability exploits, network attacks, botnet infiltration, and more (see “Selecting endpoint protection” below).




## Security technologies

- AV
- Endpoint Protection
- Multi-Factor Authentication
- Firewall
- Encryption
- Backup and Recovery
- Mobile Device Management (MGM)
- NAC (Network Access Control)
- SIEM
- Patch Management
- DLP
- EDR/EDTR

## Cybersecurity Maturity

- **Passive/Essential** – Automated actions, ad-hoc reactions on identified risks
- **Monitoring** – Automated actions, active monitoring of current state with actions reacting to alerts on attack or potential risks
- **Active-Detect and Response** – Internal data analysis and state monitoring in order to detect targeted attacks, actions according to policies intended to respond to attacks and possible attacks

## Resources

- Formal team: Full-time specialist **2-5 people**
- Dedicated: Part-time specialist **1-3 people**
- As needed: “install and forget” **0-1 people**

**Figure 4-1:** Security technologies.

## Multi-factor authentication (MFA)

MFA further enhances basic authentication (for example, username and password) by requiring an additional factor to log in to a system or application. Typically, this consists of a one-time code sent to a previously configured separate email address or via text message to a smartphone. The user must first provide their username and password. The code can only be used to authenticate a single user session within a limited time frame (for example, 60 seconds), which mitigates the effectiveness of replay attacks in which an attacker intercepts the code, then tries to use it in a separate session to authenticate. The latest form of challenge-response MFA (supported by ESET Secure Authentication) allows a user to simply confirm authentication on a paired smartphone, thereby eliminating the need to retype the one-time code.

### Firewalls

(discussed later in this chapter).

### Encryption

Encryption renders data unintelligible without the proper decryption key. Encryption and decryption can be performed in either hardware (faster) or software (less expensive). Full disk and removable media encryption protects data on servers, desktop and laptop computers, and mobile devices in the event that an endpoint is lost or stolen, or a data breach occurs. File, folder, and email encryption allow fully secure collaboration across diverse workgroups and team boundaries, with security policy enforced at all endpoints via remote central management.

### Backup and recovery

Backup and recovery systems include backup software and backup media, such as tape or disk, either on-premises (and stored off-site), remote, or in the cloud. Backups should be regularly tested to ensure that they can be recovered, and that all the necessary systems and data are being correctly backed up frequently enough to meet the requirements of the business. Backups protect businesses from accidental or malicious destruction, deletion, or modification of data (including ransomware attacks), and help to ensure business continuity in the event of a disaster.

### Mobile device management (MDM)

Many organizations, particularly SMBs, permit employees to use their personal mobile devices for work-related purposes. This popular trend is known as "bring your own device" (BYOD). However, businesses must ensure that these devices are securely operated to ensure that sensitive business information or customer data is not compromised if the device is lost, stolen, or otherwise breached. MDM software provides capabilities such as policy enforcement (for example, requiring a passcode), encryption, containerization (to isolate business apps/data from personal apps/data), and remote wipe/lock.

### Data loss prevention (DLP)

DLP software prevents accidental (or intentional) unauthorized disclosure of certain data, such as Social Security numbers, protected health information (PHI), and financial data, by scanning email and documents for certain keywords and data matching patterns.

**WARNING**

*To be effective, DLP requires additional resources to modify policies, evaluate incidents (both internal and external), and apply remedies. If DLP is deployed without this additional effort, its effectiveness will be limited.*

# SELECTING ENDPOINT PROTECTION

Endpoint protection on your desktop computers, mobile devices, and servers is your first line of defense against cyberattacks because attackers typically exploit the “weakest link” in an effort to breach your network. As such, trusting the security of your endpoints to “free” anti-malware software can be an invitation to disaster in the form of a malware infection and data breach.

Advanced endpoint protection incorporates multiple sophisticated technologies such as machine learning, pre-execution detection, sandboxing, and others in a multi-dimensional solution. Many “next-generation” endpoint protection products on the market today purport to be the “next big thing” in the fight against malware, but to be labeled “next-generation”, these products technically only have to – and often only do – implement a single facet of endpoint protection, such as machine learning. When evaluating endpoint protection for your business, look for a solution that includes ALL of the following: machine learning, pre-execution detection, sandboxing, and other leading-edge technologies, as well as traditional signature-based malware detection that is updated in real-time with cloud-based threat intelligence.

To be effective, endpoint protection must have:

**A small installation footprint**
Anti-malware software that requires significant disk space, memory resources, and processor utilization can cause performance issues and frequently be circumvented (that is, disabled) by end users.

**Robust update capabilities**
Anti-malware software must be able to get real-time threat intelligence without single points of failure or bottlenecks (such as an update server on your network). The cloud is increasingly being leveraged to deliver updates and threat intelligence to endpoints.

**Resilience**
Anti-malware software must be effective even when it is disconnected from the network and must be resistant to malware that specifically targets anti-malware.

**Product stability**
Released products should have a proven track record of being secure, stable, and free of bugs.

**Central management**
Beyond deploying endpoint protection, businesses need to be able to verify that software is correctly installed, running properly and getting regular updates. You need to be able to address endpoint protection issues remotely, and you need to be able to prove that your endpoint protection is working (for example, with logging and auditing to verify compliance).

# Securing the Network

Securing the corporate network has become much more challenging in recent years with the proliferation of mobile devices and the rise of cloud computing, but it is no less important for information security and data protection. Some examples of data protection technologies for the network include:

## Firewalls

Network firewalls remain the cornerstone of network security and are perhaps the single most important investment a business can make for network security. Basic firewalls provide packet filtering and stateful inspection of network traffic. A next-generation firewall (NGFW) provides advanced network security functionality including anti-malware protection, content filtering, intrusion detection and prevention, and threat intelligence. A web application firewall (WAF) is a type of firewall that's specifically designed to protect corporate websites and internet-facing applications.

## Intrusion detection and prevention systems (IDS/IPS)

IDS and IPS detect malicious network traffic based on preconfigured signatures and rules. An IDS is a passive system that only alerts the IT team of a possible intrusion. An IPS is an active system that can take specified actions, such as dropping or blocking malicious traffic.

## Software as a Service (SaaS)

SaaS applications have become ubiquitous as users readily find and install easy-to-use software to help them perform their daily business functions. Examples of popular SaaS applications include Box, Dropbox, Google Docs, OneDrive, and others. Businesses need to actively identify SaaS applications that are being used on their network and either sanction (and educate about) the use of specific SaaS apps, or explicitly block them.

## VLAN segmentation

Virtual local area network (VLAN) segmentation logically segments a network, for example, by departments (such as finance, human resources, and operations) to prevent unauthorized access to certain data and to prevent excessive network traffic (for example, broadcast storms) that may cause slow performance.

## Virtual private network (VPN)

A VPN appliance or software enables remote users to connect to the corporate network over the internet using an encrypted tunnel. A VPN can also be used to connect partner and/or provider networks, such as a vendor in your supply chain or a cloud service provider.

## Network access control (NAC)

NAC is a unified security management solution that enforces security policies based on user or system authentication, allowing access to certain parts of the network depending on the system or user's compliance with security policies (for example, security patches and antivirus signatures are current, network connection is encrypted using a VPN, and so on).

### Security information and event management (SIEM)

SIEM solutions aggregate and analyze log information from numerous data sources such as firewalls, IDS/IPS, WAFs, servers, and endpoints.

### Patch management

Patching known security vulnerabilities on servers and endpoints is a critical security function for all organizations. As the size of your organization grows, manually installing software patches on hundreds of servers and endpoints that may be spread across multiple remote locations becomes increasingly difficult. Patch management solutions help organizations automate and manage many patch management functions.

### Password managers

It's simple but powerful – implementing password managers throughout the company is very worthwhile.

### Domain Name System (DNS) protection

DNS has re-emerged as a popular attack vector, particularly for denial-of-service (DoS) attacks. Security enhancements to the DNS protocol – such as DNS Security Extensions (DNSSEC) as well as DNS server configuration security best practices (such as disabling recursive lookups) need to be implemented. Other DNS security options include installing dedicated (and hardened) DNS appliances or using a managed DNS service.

### Web content filtering

Content filtering prevents users from visiting unauthorized and potentially harmful or malicious websites based on the website address (IP address or URL) or actual content.

## Understanding the Need for Orchestration

As your business grows, the need for automation and orchestration in your IT processes becomes increasingly important, particularly if you have a small IT staff with limited resources. Manually installing and configuring endpoints – desktop PCs, mobile devices, and servers – is unsustainable in a growing business, particularly across multiple remote locations.

Beyond the inefficiencies associated with "touching" every endpoint, manual processes introduce opportunities for mistakes such as inconsistent or misconfigured settings.

Automation and orchestration improve efficiency in your IT team, increase productivity for your end users (by reducing downtime), and reduce potentially costly configuration errors. Management platforms can help to automate manual processes and set standard policies.

**TIP**

*For SMBs that lack the resources to deploy an on-premises management platform, a cloud-based solution or managed service provider (MSP) can provide the automation and orchestration services needed to support rapid growth and an increasingly complex IT environment.*

# ESET DELIVERS PROTECTION FOR ON-PREMISES, REMOTE, AND MOBILE ENDPOINTS

Mercury Engineering is Ireland's largest engineering company, employing around 4,000 employees, including a large mobile workforce that often works remotely in over 30 countries in diverse and challenging operating environments. Many employees connect to unsecure networks such as public Wi-Fi and cellular networks.

## Challenges

Mercury's main IT focus is ensuring the security of data in these potentially dangerous environments. The company's commercial information is essential to its growth – tender and estimation data is critical to acquiring and maintaining clients. The security of this information is vital to the company. The health of individual machines is also extremely important to Mercury. Many of their staff work to very tight deadlines and operate PCs with custom software/hardware setups which cannot be quickly replaced if compromised.

Previous anti-malware products at Mercury failed to stop several malware infections and serious virus outbreaks. Staff were frequently locked out of their computers and Mercury's helpdesk spent a lot of time treating different malware infections, often resorting to various freeware anti-malware products that lacked the management, scalability, and reporting capabilities of a business-grade solution. The backend was very complex, difficult to manage, maintenance-heavy, and expensive – professional services were needed to help when changes or upgrades were required. The monitoring and management solution was very limited in its functionality, especially on remote endpoints outside of the network. There was a lack of real-time awareness of what was happening on Mercury's endpoints – finding out about an outbreak at the end of the day was often too late to prevent further spread of the damage. Their old anti-malware products had them working overtime to make up for the shortcomings of the software.

## Solution

When Mercury moved to ESET, the process was fast. It was "deployed within hours rather than days". Implementation was also straightforward: the new network was rolled out entirely by one Mercury system administrator (with some technical support from ESET Ireland). The entire ESET network is now administered from one small machine with just one processor and 4 gigabytes (GB) of memory that supports the management of over 1,000 computers and 200 servers in various countries, plus public networks all over the world. It also ensures that Mercury's security complies with international standards and mandates, such as ISO 27001.

"For the end user, there's no impact, they don't know that it's happening – it runs so quietly and efficiently in the background. Day-to-day business continues as normal and we continue to be protected without the end user being affected in any shape or form. The best testimony? The stats from our helpdesk: after we introduced ESET, our support guys don't log any calls – they don't have to deal with any antivirus or malware-related issues!" says Mercury's IT Infrastructure Manager.

## Results

- More than four years completely free of malware and virus problems
- Unobtrusive profile and a small footprint of the ESET solution
- Real-time monitoring for immediate threat mitigation and remediation
- Manages remote and mobile endpoints outside of the corporate network
- Helps secure confidential information such as tenders and estimation data

TIP

*Many SMBs use ESET Security Management Center (ESMC) and ESET Cloud Administrator (ECA) to easily and securely manage their remote and cloud resources, respectively, without requiring costly and complex on-premises hardware deployments.*

**In This Chapter**

- Complementing technical controls with organizational controls
- Recognizing the need for process controls

Chapter 5

# EXPLORING ORGANIZATIONAL AND PROCESS CONTROLS

*In this chapter, you'll learn how organizational and process controls work together with technical controls to help your business to protect data.*

## Establishing Organizational Controls

Effective data protection requires more than technical solutions. You need to establish administrative and organizational controls to ensure that technical controls are properly deployed, configured, and operated in support of a cohesive security management strategy. Some examples of organizational controls include:

### Private and sensitive personal data

Technical controls, such as encryption and data loss prevention (DLP) software, need to be used with discretion due to their costs (both financial and performance-related). Encryption requires additional processing to encrypt and decrypt data, and DLP solutions need to scan for keywords and patterns to identify private or sensitive data such as credit card numbers, health information, and Social Security numbers. Establishing a data classification scheme can help your users understand what data needs to be protected, why, and how.

### Data documentation and auditing

Businesses that collect, process, and/or store sensitive data need to document why they collect that data, how it's collected (what are the sources), how it's used, and how it's protected. Documenting your data security and data privacy policies can help you address these questions and satisfy audit requirements, particularly with regard to regulations such as the US Health Insurance Portability and Accountability Act (HIPAA) and the EU General Data Protection Regulation (GDPR).

## Security policies

Policies don't need to be extensive tomes. In many cases, a few paragraphs may be all that's needed. Security policies should clearly define individual roles and responsibilities as they relate to the protection of personal data. Examples of important security policies that every business should create include:

- Internet and email acceptable use policy
- Bring your own device policy
- Remote access policy
- Authorized software policy

## Human resources

This includes policies and procedures to ensure that personal data (such as employment applications, payroll data, training, and disciplinary records) that is collected, maintained, and processed by human resources is properly protected. This also includes processes such as pre-employment screening, drug testing, and job rotations.

## Using a security maturity model

A security maturity model can help you determine your security capabilities in specific areas and identify any gaps between where you are and where you need to be. Where you need to be will, of course, depend on a number of factors such as:

- What you are protecting – such as sensitive data, financial information, intellectual property, medical equipment, or critical infrastructure.
- Your industry – such as medical, financial, retail, defense contracting, or public utilities.
- Your regulatory compliance requirements – for example, are you subject to the US Health Insurance Portability and Accountability Act (HIPAA), EU General Data Protection Regulation (GDPR), Canada Personal Information Protection and Electronic Documents Act (PIPEDA), Payment Card Industry Data Security Standards (PCI DSS), or others?
- Your threat profile – are you geographically located in a hostile or unstable region, high-crime city, or hazardous or industrial area?

## Training and testing your employees

Security awareness training for all of your employees is necessary to ensure that your employees aren't the weakest link when it comes to data protection in your organization. You need to cover topics such as password security, spam and phishing, malware protection, compliance requirements, and data protection (such as data classification, types of sensitive data, and data protection technologies). Testing can take many forms to ensure that training is engaging and reinforced throughout the year.

## Performing data protection impact analysis (DPIA)

DPIA is required by GDPR for any data processing operations that are "likely to result in a high risk to the rights and freedoms of individuals." A DPIA is similar to the basic risk management process (discussed in Chapter 2), but further defines additional parameters that are related to processing personal data.

## Implementing data protection by design and by default

The GDPR requires "data protection by design and by default", meaning organizations should implement technical and organizational measures to minimize personal data that is collected, processed, and stored by an organization.

# DATA PROTECTION FROM A TO Z (WELL, TO F)

The following systematic approach to cybersecurity can help you to protect valuable data in your business. It's as simple as A, B, C … D, E, F!

## ASSESS your assets, risks, and resources

List all of the computer systems and services that your business uses. After all, if you don't know what you have, you can't protect it. Be sure to include mobile devices such as smartphones and tablets that may be used to access company or customer information. This is particularly important because, according to the Ponemon Institute, it's estimated that 60 per cent of employees circumvent security features on their mobile devices, and 48 per cent of employees disable their employer-required security settings. And don't forget cloud services, such as Box, Dropbox, iCloud, Google Docs, Office365, OneDrive, and SalesForce.

Next, review your list and consider the risks associated with each item as well as whether or not you actually still need the system, software, or service. Who or what is the threat? Another good question to ask is: "What could possibly go wrong?" Some risks are more likely to occur than others, but list them all and then rank them according to how much damage they could cause and the likelihood that they might occur.

You might need outside help with this process, which is why you need another list: the resources you can tap for cybersecurity issues. This could be someone on the staff who's knowledgeable and security-savvy, or a partner or vendor. National trade groups and local business associations also have resources and can provide helpful advice. The National Cyber Security Alliance provides free educational materials, tip sheets, and employee training suggestions. Plus, be sure to check in with your local law enforcement office (you should at least have contact names and numbers to call in case you're the victim of a cybercrime).

## BUILD your policies

A sound security program begins with security policies that have executive buy-in. If you're the boss, you need to let everyone know that you take security seriously and that your company is committed to protecting the privacy and security of all the data that it handles. Next, you need to spell out the policies that you want to enforce, for example, there shall be no unauthorized access to company systems and data, and employees will not be allowed to disable the security settings on their mobile devices.

## CHOOSE your controls

You use controls to enforce policies. For example, to enforce the policy of no unauthorized access to company systems and data, you may choose to control all access to company systems with a unique username, password, and token.

To control what programs are permitted to run on company computers, you may decide not to give employees administrative rights. To prevent breaches caused by lost or

stolen mobile devices, you could require employees to report such incidents on the same day and specify that such devices will be remotely locked and erased immediately.

As a minimum, you need three basic security technologies:

- **Anti-malware software** that prevents malicious code (such as viruses and ransomware) from being downloaded onto your devices.
- **Encryption** that renders data on lost or stolen devices inaccessible.
- **Multi-factor authentication** so that more than a username and password (such as a one-time passcode sent to a registered mobile phone) is required to gain access to your systems and data.

### DEPLOY controls

When you deploy controls, make sure that they work. For example, you can have a policy that prohibits unauthorized software on company systems; one of your controls will be anti-malware software that scans for malicious code. You need to install this and test that it doesn't interfere with normal business operations, and document the procedures to follow when malware is detected.

### EDUCATE employees, partners and vendors

Your employees need to know more than just the company security policies and procedures. They also need to understand why these are necessary. This means investing in security awareness and education, which is often the single most effective security measure you can implement.

By working with your staff, you can raise awareness of issues such as phishing email. A recent Verizon Data Breach Investigations Report (DBIR) showed that 23 per cent of phishing emails sent to employees were opened and 11 per cent of recipients opened an attachment, both of which greatly increase the chances of data breach and information theft.

Educate everyone who uses your systems, including executives, vendors, and partners. And remember that violations of security policies must have consequences. Failure to enforce policies undermines the whole security effort.

### FURTHER assess, audit, and test

Cybersecurity for any business, large or small, is an ongoing process, not a one-time project. Plan on reassessing your security on a periodic basis, at least once a year. Stay up-to-date on emerging threats by reviewing security news on a regular basis via websites such as WeLiveSecurity.com, KrebsOnSecurity.com and DarkReading.com.

You may need to update your security policies and controls more than once a year depending on changes to the business, such as new vendor relationships, new projects, new hires, or employees departing (including making sure that all system access is revoked when anyone leaves the company). Consider hiring an outside consultant to perform a penetration test and security audit to find out where your weak points are and then address them.

# Looking at Process Controls

Process controls help businesses to minimize the impact of a data breach or data loss. For example, a recent study by the Ponemon Institute found that businesses can reduce the average per-record cost of a data breach from an average of $141 to approximately $122 if an effective incident response process is implemented to help reduce the time it takes to identify and contain a data breach. Your incident response team can be in-house, an outsourced third-party partner, or a combination of both. For a breach of just 10,000 records, that represents average savings of approximately $190,000 – well worth the investment.

When creating process controls, businesses need to:

### Involve people

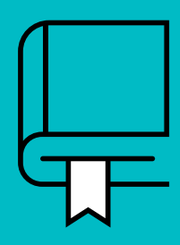
This shouldn't be a top-down management initiative. Involving the people that actually work with the various processes and technology will help to ensure that the controls make sense and can be effectively implemented.

### Define responsibilities

Individual responsibilities need to be clearly defined and understood: everyone needs to know their role.

### Explain why process controls are needed

Security measures are often seen as a burden or a hindrance. They may ultimately be ignored or circumvented if employees don't understand why the controls are needed and why they are important to the business.



REMEMBER

*According to the Ponemon Institute, the average time it takes to identify a data breach is 191 days, and the average time to contain a data breach is 66 days. The amount of time required to identify and contain a data breach directly impacts the size of the data breach and its total cost.*

Businesses that create processes for secure data transfer can also reduce the cost of a data breach or data loss. For example, encryption reduces the average per-record cost by $16, according to the Ponemon Institute. In many cases, encrypting data (and being able to prove that it's properly encrypted) can trigger safe harbor provisions for many data privacy regulations. Doing so enables businesses to forgo breach notifications, which significantly reduces the cost – both in terms of direct costs (such as notifications, credit monitoring services, and litigation) and indirect costs (such as brand damage and customer churn). Again, in the case of a breach of 10,000 records, encryption can reduce the total cost of the breach by approximately $160,000.

Important process controls include:

### Access control policies

Defines who has access to which systems, applications, and data, and for what purposes.

### Resource/asset management

It's important to know what you're protecting and why (its value or risk to the organization). Beyond keeping an accurate inventory of computing and data assets/resources, organizations need to ensure proper security hygiene – keeping systems and applications updated with the latest security patches and promptly deleting or destroying sensitive data that is no longer required, in accordance with established data retention, archiving, and destruction policies.

### Change management

Ensures changes to systems and applications are documented, tested, and approved, so that the impact of a change is understood as it relates to the organization's overall security posture.

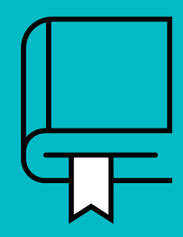
### Incident response

When a security incident (such as a data breach or attack) occurs, businesses need to have a clearly defined and well understood incident response plan. This helps to ensure a prompt and effective response, including damage containment, recovery, preservation of evidence, internal and external communications, and root cause analysis.

### Business continuity

A business continuity plan minimizes the business impact of an outage or disaster, helping businesses to continue functioning until normal operations can be fully resumed.

Finally, businesses can leverage professional security services to supplement in-house capabilities. This includes day-to-day monitoring and threat intelligence, as well as detection, escalation, and incident response. This is particularly important in forensic and investigative activities, assessment and audit services, crisis team management, and communications.



REMEMBER

*The organizational and process controls that are implemented should be appropriate to the level of risk.*

**In This Chapter**

- Getting started with administrative controls
- Knowing what you're protecting and how to protect it
- Implementing technical controls
- Ensuring backup and recovery, incident response, and disaster recovery
- Working with your users and other security experts

Chapter 6

# TEN KEYS TO EFFECTIVE DATA PROTECTION

*In this chapter, we provide ten security best practices to help you to ensure effective data protection for your business.*

## Create security policies

Many companies dismiss the importance of written security policies and go straight to the technical controls. Technical controls (such as firewalls, endpoint protection, and so on) implemented without administrative controls (that is, policies and procedures) are almost always implemented in a reactive manner without a thoughtful, cohesive, and comprehensive security strategy, and security management framework (which your policies, along with information security analysis, help to define). This inevitably means that you'll spend too much on technical solutions that aren't effectively (or correctly) deployed and provide incomplete or inadequate protection.

## Identify your assets

You need to know what you're protecting, so it's important to maintain an accurate inventory of all your IT hardware and software. Without a complete inventory, you may not be aware of vulnerable systems in your network that can increase your attack exposure. For example, in the 2013 Target data breach, attackers remotely accessed a heating, ventilation, and air conditioning (HVAC) maintenance system to eventually breach the credit/debit card and/or personal information of 110 million customers. There are plenty of freely available tools you can use to scan your network and endpoints to get started. Commercial solutions can help you to accurately maintain your asset inventory on an ongoing basis, and many also provide remote management capabilities to help you to install, remove, and update software as well. You need to reduce the attack surface for all of your internet-connected assets (including personal mobile devices), by installing and maintaining appropriate security protection.

## Know your security posture

This is as simple as creating a roadmap or maturity model to show where you are today (your current state) and using a risk-based approach to identify relevant threats against the assets in your environment (see the previous tip) and the appropriate cybersecurity and data protection measures. You can then perform a gap analysis and determine what steps you need to take and where to invest your resources. Refer to Chapter 3 for more about assessing data security risks.

## Classify all of your data

For many businesses, sensitive customer data and other proprietary information represents the "crown jewels" of the business, but providing equal protection and controls for all of your data throughout its lifecycle is neither practical nor desirable. Instead, think about which data would keep you up at night if it were lost or stolen. How would a data breach impact your brand image, customer loyalty, or even the ongoing viability of your business? Create (and document) an intuitive data classification policy for your organization that includes classification labels (such as "Internal Use Only," "Sensitive Data," and "Approved for Public Release") and that specifies data protection requirements (such as encryption, backups, release approval, and destruction) for different levels of information.

TIP

*The General Data Protection Regulation (GDPR) requires organizations to delete personal data if requested by a subject (such as an individual). To help you comply with GDPR requirements, design your data classification strategy to help you identify or flag personal data (including backups) that may need to be deleted or otherwise altered in the future.*

## Encrypt your sensitive data

Data encryption converts plain text data to an unreadable form (known as "ciphertext"), rendering it useless to unauthorized parties who don't possess the encryption/decryption keys. Thus, the key to effective encryption is to properly secure the keys. At a minimum, you should encrypt data "at rest" (in storage). You can use additional encryption on data "in motion" (or "in transit"), for example, using Secure Sockets Layer (SSL) encryption. Finally, for data "in use," you should take advantage of encryption within the application, if available. Encryption can be either hardware- or software-based.

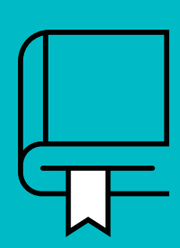
TIP

*Many data breach regulations include safe harbor provisions for data that's encrypted, which can significantly reduce the cost and impact of a data breach.*

## Backup and (test) recover your valuable data

Ensuring regular and reliable backups of your systems and data is a basic, but essential, security best practice. Good backups ensure that you can recover a file that's accidentally deleted, or a hard drive that's corrupted. With disk-based backup costs

continuing to drop and cloud-based backup solutions being cost-effective and easy to use, there's simply no excuse for not having backups. With the rapid rise of ransomware over the past several years, backups are the only way you're guaranteed to get your data back if you're the victim of a ransomware attack. As a bonus, you won't need to pay the ransom.



REMEMBER

*You need to regularly test your ability to recover your critical systems and data from backups, not only to ensure that the backups aren't corrupted, but also to verify that you and your staff know the recovery process.*

## Invest in endpoint protection

"Invest" doesn't mean downloading some free antivirus software from the internet it means protecting all of your endpoints – desktop PCs, mobile devices, and servers – with a robust commercial endpoint protection solution. Today, information is everywhere and now, more than ever, the endpoint is where everything comes together. So it's definitely an area worth investing in.

## Plan and prepare

Every business needs to have an incident response plan, business continuity and disaster recovery plans. Your incident response team needs to be trained in basic forensic procedures to ensure that every security incident is treated as a potential legal case and ensure that the chain of custody is maintained for any potential evidence. Business continuity and disaster recovery plans help your business to resume normal business operations as quickly as possible after a major event or disaster. Accurate and timely communications, both internal and external, are a critical component of any business continuity and disaster recovery plans.

## Train your users

The weakest link in any organization's security has always been the end user, but that's not necessarily their fault. It's unlikely that everyone who works for your business was hired because they're security experts. Attackers know this and use social engineering techniques to lure unsuspecting users to click malicious links in spam or phishing emails, reveal their passwords (see "How do you create a strong password?" below), and visit malicious websites, among other tactics. Conduct regular, engaging, relevant and short security awareness training exercises to help your users to help themselves – and therefore help you!

## Don't "go it alone"

Cybercriminals don't work alone. They work with other dubious characters to achieve their attack objectives, reuse malicious code on the dark web, and enlist unsuspecting victims whose breached endpoints have become bots in a botnet army targeting other victims. But the good guys aren't alone either. Leverage the broad community of security experts from local law enforcement to professional associations, outsourced and managed security services, real-time cloud-based threat intelligence, and more.

# HOW DO YOU CREATE A STRONG PASSWORD?

Almost everything we do online requires a login, and every login requires some kind of authentication to verify that we are who we say we are. As such, your password should be as unique (and complex) as you are! Here are a few tips:

**DO use long passwords and passphrases**

Passwords should be at least 8 characters long, but not so long that you can't remember them (see the tip below). Check that your password hasn't been exposed in a data breach at https://haveibeenpwned.com/Passwords.

**DO use unique phrases and special characters**

A short phrase consisting of 30 or more characters (perhaps with some numbers, capitalization and punctuation) that you can remember is far better than an 8-character word with common substitutions (like a '3' for the letter 'e').

**DO use a password manager program (free or paid)**

A password manager can be helpful for creating, storing, managing, and remembering unique, strong passwords for your various device, system, and application logins. It can also help to eliminate the common practice of writing down passwords in documents or on sticky notes.

**DO use passwords you can remember**

Overly complex, completely random passwords that are difficult to remember can actually be counterproductive and make your account less secure, because it tends to lead to bad practices such as writing down passwords and using the same passwords across different personal and work accounts.

**DO use multi-factor authentication (MFA)**

When possible, MFA should be enabled on your accounts instead of, or in addition to, passwords. MFA incorporates two or more authentication factors ("something you know," such as your username and/or password, and "something you have," such as a hardware or software token, or a smartphone). When you log into an MFA account, a one-time code is generated on your token or sent via SMS text message to your smartphone. The code can only be used one time, and only within a limited period of time (typically within one to five minutes). This makes it extremely difficult for an attacker to intercept your code and use it to log into your account without your knowledge and before the code expires.

**DO NOT use the same password twice, regardless of how good it is**

If your password gets compromised in one place (say, your personal Yahoo! email account), cybercriminals will try to use those same credentials in other places (like your online bank account).

**DO NOT share your passwords with anyone – ever!**

Treat your passwords as more sacred than your toothbrush (which you might occasionally share with your significant other – or your dog).

**DO NOT use common dictionary words**

Automated password cracking programs make easy work of dictionaries – including foreign languages and medical, legal or engineering terms. Also avoid repetitive characters (for example, 'aaaa'), sequential characters (for example, '1234'), and recognizable patterns (for example, 'qwerty').

**DO NOT use personal information in your password**

Social media makes it easier than ever for cybercriminals to learn personal details about you – including your middle name, birthdate, address, school, spouse's or child's name, and what you did last summer!

# GLOSSARY

**adware**

Pop-up advertising programs that are commonly installed with freeware or shareware, and sometimes considered to be a form of malware. See also malware.

**backdoor**

Malware that enables an attacker to bypass normal authentication to gain access to a compromised system. See also malware.

**bootkit**

A kernel-mode malware variant of a rootkit, commonly used to attack computers that are protected by full-disk encryption. See also malware and rootkit.

**bot**

A target computer that is infected by malware and is part of a botnet. See also botnet and malware.

**botnet**

A broad network of malware-infected bots working together and controlled by an attacker through command-and-control (C2) servers. See also bot and malware.

**bring your own device (BYOD)**

A mobile device policy that permits employees to use their personal mobile devices, such as smartphones and tablets, in the workplace for both work-related and personal use.

**ciphertext**

A plaintext message that has been encrypted into a scrambled message that is unintelligible without the proper decryption key. See also decryption, encryption, and plaintext.

**cryptocurrency**

A digital asset that uses cryptography to secure transactions, control the creation of additional units, and verify the transfer of assets. Bitcoin is a popular example of cryptocurrency.

**decryption**

The process of transforming ciphertext into plaintext. See also ciphertext and plaintext.

**directory harvest attack (DHA)**

A brute force technique used by spammers in an attempt to find valid email addresses in a domain.

### distributed denial-of-service (DDoS)

A large-scale attack that typically uses bots in a botnet to crash a targeted network or server. See also bot and botnet.

### DNS cache poisoning

A type of attack, also known as DNS spoofing, that exploits vulnerabilities in DNS to divert internet traffic away from legitimate destination servers to fake servers. See also Domain Name System (DNS).

### DNS hijacking

An attack technique used to redirect DNS queries away from legitimate DNS servers. See also Domain Name System (DNS).

### Domain Name System (DNS)

A decentralized hierarchical database for computers, services, and other resources connected to a network or the internet which provides mapping of numerical IP addresses to domain names, as well as other information. See also Internet Protocol (IP).

### drive-by download

Software, often malware, downloaded onto a computer from the internet without the user's knowledge or permission. See also malware.

### encryption

The process of transforming plaintext into ciphertext. See also ciphertext and plaintext.

### endpoint

An end-user computing device, such as a desktop or laptop computer, tablet, or smartphone.

### exploit

Software or code that takes advantage of a vulnerability in an operating system (OS) or application, and causes unintended behavior in the OS or application, such as privilege escalation, remote control, or a denial-of-service.

### General Data Protection Regulation (GDPR)

Applicable to any organization that does business with EU citizens. Strengthens data protection for EU citizens and addresses the export of personal data outside the EU.

### Health Insurance Portability and Accountability Act (HIPAA)

Applicable to any organization that processes or stores protected health information (PHI). Protects patient confidentiality and data privacy.

### International Organization for Standardization (ISO)

An international body for creating standards. ISO is derived from the Greek word 'isos', meaning equal.

**internet protocol (IP)**
The principal communications protocol in the TCP/IP communications suite for routing across network boundaries (routers) and the internet. See also Transmission Control Protocol (TCP).

**intrusion detection system (IDS)**
A hardware or software application that detects suspected network or host intrusions.

**intrusion prevention system (IPS)**
A hardware or software application that detects and blocks suspected network or host intrusions.

**logic bomb**
A malware program, or portion thereof, designed to perform some malicious function when a predetermined circumstance occurs. See also malware.

**malware**
Malicious software or code that typically damages or disables, takes control of, or steals information from a computer system. Malware broadly includes viruses, worms, Trojan horses, logic bombs, ransomware, rootkits, bootkits, backdoors, spyware, and adware.

**metamorphism**
A technique used to rewrite malware code with each iteration so that each new version is different from the preceding version. See also malware and polymorphism.

**next-generation firewall (NGFW)**
A network security platform that fully integrates traditional firewall and network intrusion prevention capabilities with other advanced security functions that provide deep packet inspection (DPI) for complete visibility, accurate application, content, and user identification, and granular policy-based control. See also intrusion prevention system (IPS).

**Payment Card Industry (PCI) Data Security Standards (DSS)**
Applicable to any business that accepts, processes, or stores payment cards (such as credit, debit, and cash card) transactions.

**Personal Information Protection and Electronic Documents Act (PIPEDA)**
Applicable to organizations that do business with Canadian citizens. Protects the privacy of personal information for Canadian citizens.

**phishing**
A social engineering technique in which an email that appears to be from a legitimate business (such as a financial institution) attempts to trick the recipient into clicking an embedded link in the email or opening an attachment containing malware or an exploit.

The embedded link redirects the recipient's browser to a malicious website to enter sensitive personal information (such as account information). Alternatively, the malicious website may deliver malware or an exploit to the victim's endpoint in the background via the browser. See also drive-by download, endpoint, exploit, and malware.

### plaintext

A message in its original readable format or a ciphertext message that has been properly decrypted to produce the original readable message. See also ciphertext and decryption.

### polymorphism

A technique used to rewrite a portion of malware code with each iteration so that each new version is slightly different from the preceding version. See also malware and metamorphism.

### port hopping

A technique used by applications to improve accessibility, but also used in cyberattacks to dynamically switch TCP ports to evade detection. See also Transmission Control Protocol (TCP).

### protected health information (PHI)

Any information about the health, provisioning of healthcare, or payment for healthcare that is created or collected by an organization, such as a healthcare provider, insurer, or other such entity, that can be linked to a specific individual.

### ransomware

Malicious software that encrypts a victim's data and instructs the victim to pay a specified ransom (usually in cryptocurrency) to decrypt the data (although payment of a ransom does not guarantee that the victim's data will be decrypted). See also cryptocurrency and malware.

### remote access Trojan (RAT)

A malware program that includes a backdoor to provide administrative control of a target computer.

### rootkit

Malware that provides privileged (root-level) access to a computer. See also malware.

### Secure Sockets Layer (SSL)

A transport layer protocol that provides session-based encryption and authentication for secure communication between clients and servers on the internet.

### social engineering

A low-tech attack method that employs techniques such as shoulder surfing and dumpster diving to obtain sensitive information, such as passwords, from a user.

### spam

Unsolicited bulk email that is commonly used to spread malware via malicious links or attachments. See also malware.

### spearphishing

A targeted phishing attempt that seems more credible to its victims and thus has a higher probability of success. For example, a spearphishing email may spoof an organization or individual that the recipient knows. See also phishing.

### spyware

Malware that gathers information about a person or organization without their knowledge or consent. See also malware.

### SSL hiding

A technique that uses SSL (Secure Sockets Layer) encryption to hide the contents of network traffic, for example, to evade detection by network defenses while stealing sensitive data (known as data exfiltration).

### Transmission Control Protocol (TCP)

One of the core protocols of the internet Protocol suite, TCP is one of the two original components of the suite, complementing the internet Protocol (IP), and therefore the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. TCP is the protocol that major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on. See also Internet Protocol (IP).

### Trojan horse

A malware program that purports to perform a given function, but instead performs some other (usually malicious) function. See also malware.

### unified threat management (UTM)

A security appliance that integrates various security features such as firewall, anti-malware, and intrusion prevention capabilities into a single platform.

### Uniform Resource Locator (URL)

A web address.

### virtual local area network (VLAN)

A broadcast domain that is partitioned and isolated in a local area network.

### virtual private network (VPN)

A private network used to communicate privately over public networks. VPNs utilize encryption and encapsulation to protect and simplify connectivity.

**virus**

A set of computer instructions whose purpose is to embed itself within another computer program in order to replicate itself. See also malware.

**vulnerability**

A bug or flaw in software that creates a security risk which may be exploited by an attacker. See also exploit.

**web application firewall (WAF)**

A firewall designed to protect web-based applications and web servers.

**worm**

Malware that usually has the capability to replicate itself from computer to computer without the need for human interaction. See also malware.

# YOUR DATA IS YOUR BUSINESS

## MAKE SURE YOUR COMPANY IS SAFE FROM DATA BREACHES OR LEAKS. EMPLOY OUR POWERFUL, EASY TO DEPLOY ESET ENDPOINT ENCRYPTION

- ✔ Safely encrypt hard drives, removable media, files and email
- ✔ Boost your information security and comply with the GDPR
- ✔ Add an additional security layer with ESET Secure Authentication

**VISIT THE ESET WEBSITE FOR ALL OUR SOLUTIONS.**

CYBERSECURITY
EXPERTS ON YOUR SIDE

**WWW.ESET.COM**

**CYBERSECURITY**
**EXPERTS ON YOUR SIDE**

**WWW.ESET.COM**



We gratefully thank Lawrence Miller for content preparation of this e-book.